



DRM Architecture

Draft Version 2.0 – 01 Sept 2003

Open Mobile Alliance
OMA-DRM-ARCH-V2_0-20030901-D

Use of this document is subject to all of the terms and conditions of the Use Agreement located at <http://www.openmobilealliance.org/UseAgreement.html>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the “OMA IPR Declarations” list at <http://www.openmobilealliance.org/ipr.html>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE “OMA IPR DECLARATIONS” LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2003 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

- 1. SCOPE2
- 2. REFERENCES2
 - 2.1 NORMATIVE REFERENCES2
 - 2.2 INFORMATIVE REFERENCES2
- 3. TERMINOLOGY AND CONVENTIONS2
 - 3.1 CONVENTIONS2
 - 3.2 DEFINITIONS.....2
 - 3.3 ABBREVIATIONS2
- 4. INTRODUCTION2
 - 4.1 ACTORS AND FUNCTIONAL ENTITIES2
 - 4.2 FUNCTIONAL ARCHITECTURE2
 - 4.3 TECHNICAL USE CASES2
 - 4.3.1 Basic Pull Model.....2
 - 4.3.2 Push of Protected Content.....2
 - 4.3.3 Streaming of Protected Content2
 - 4.3.4 Backup2
 - 4.3.5 Super Distribution.....2
 - 4.3.6 Export2
 - 4.3.7 Store and Forward.....2
- 5. TRUST AND SECURITY MODEL2
 - 5.1 OVERVIEW.....2
 - 5.2 TRUST MODEL.....2
 - 5.3 CONTENT PROTECTION2
 - 5.4 RIGHTS OBJECT2
 - 5.5 RIGHTS OBJECT PROTECTION.....2
 - 5.6 OTHER SECURITY ASPECTS.....2
- APPENDIX A. CHANGE HISTORY (INFORMATIVE)2
 - A.1 APPROVED VERSION HISTORY2
 - A.2 DRAFT/CANDIDATE VERSION 2.0 HISTORY2

Figures

- Figure 1. Functional architecture.....2

1. Scope

The scope of OMA “*Digital Rights Management*” is to enable the controlled consumption of digital media objects by allowing content providers the ability, for example, to manage previews of protected content, to enable superdistribution of protected content, and to enable transfer of content between DRM agents. The OMA DRM specifications provide mechanisms for secure authentication of trusted DRM agents, and for secure packaging and transfer of usage rights and DRM protected content to trusted DRM agents.

2. References

2.1 Normative References

None

2.2 Informative References

[DRMREQ]	OMA DRM Requirements Version 2.0. Open Mobile Alliance™. OMA-DRM-REQ-V2_0-20030425-d
[OMADRM]	OMA DRM Specification V 2.0. Open Mobile Alliance™. OMA-DRM-DRM-V2_0-2003xxxx-d
[OMADCF]	OMA DRM Content Format V 2.0. OMA Open Mobile Alliance™. OMA-DRM-CF-V2_0-2003xxxx-d
[OMAREL]	OMA DRM Rights Expression Language V 2.0. Open Mobile Alliance™. OMA-DRM-REL-V2_0-2003xxxx-d
[ISO 7498-2]]	ISO/IEC 7498: Information processing systems -- Open Systems Interconnection -- Basic Reference Model - Part 2: Security Architecture
[MPEG21 RDD]	ISO/IEC CD 21000-Part 6 - Rights Data Dictionary (RDD) (2002-07-26)
[ODRL 1.1]	Open Digital Rights Language (ODRL), Version: 1.1 (2002-08-08), http://odrl.net

3. Terminology and Conventions

3.1 Conventions

This is an informative document, which is not intended to provide testable requirements to implementations.

3.2 Definitions

Actor	An actor is an external entity that carries out use cases.
Backup	Defines an action for duplicating a Media Object and/or Rights Object and transferring them to another location that is not a Device.
Billing Service Provider	The entity responsible for collecting payment from a User.
Composite Object	A Media Object that contains one or more Media Objects by means of inclusion e.g. DRM messages, zip files.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities or processes. (From [ISO 7498-2])
Content	One or more Media Objects
Content Issuer	The entity making content available to the DRM Agent; the entity whose Content is being Protected.
Content Provider	An entity that is either a Content Issuer or a Rights Issuer.
Copy	To make a perfect reproduction of Protected Content or a Rights Object.
Device	A Device is a user equipment with a DRM Agent. The Device MAY include a smartcard module (e.g. a SIM) or not depending upon implementation.
DRM Agent	The entity in the Device that manages Permissions for Media Objects on the Device.
DRM Message	A message containing a Media Object and optionally, a Rights Object. Media objects received inside a DRM Message must not leave the Device. The optional Rights Object defines Permissions for the Media Object.
Enable	To make a resource (Media Object) capable of being interacted with. When applied to a digital resource, Enable results in a change in an existing resource such that it becomes capable of being read, written to or executed. Enabling MAY be partial and/or contextual. (From [MPEG21 RDD])
Execute	To execute a software programme
Functional Entity	Internal building block of the architecture.
Integrity	The property that data has not been altered or destroyed in an unauthorised manner. (ISO 7498-2)
Media Object	A digital work e.g. a ringing tone, a screen saver, a Java game or a Composite Object.
Network Service Provider	The entity providing network connectivity for a mobile Device.
Network Store	An entity remote to the device and controlled by a service provider which can store Protected Content and encrypted Rights Objects on behalf of a Device for Backup.
OMA DRM Conformant Device	A Device that will work interoperably with other OMA DRM Conformant Devices and some or all of the following; Billing Service Providers, Content Providers and Network Service Providers. It will also enable Protected Content on the Device only if the Device possesses a valid Rights Object for that instance of Protected Content and only according to the Permissions defined in the Rights Object for that instance of Protected Content.
Permission	Actual usages or activities allowed (by the Rights Issuer) over Protected Content (From [ODRL 1.1])
Play	To create a transient, perceivable rendition of a resource (From [MPEG21 RDD])
Print	To create a fixed and directly perceivable rendition of a resource (From [MPEG21 RDD])
Protected Content	Media Objects that are consumed according to a set of Permissions in a Rights Object.
Restore	Defines an action for duplicating a Media Object and/or Rights Object, transferring it back to the Device from which it was Backed up and then deleting the Rights Object from the backup location if applicable. .

Revoke	A Device has been Revoked by a particular Rights Issuers if that Rights Issuers has decided it does not wish to issue Rights Objects to that Device (for example, because it has concerns about the robustness of the Device's implementation).
Rights Issuer	An entity that issues Rights Objects to OMA DRM Conformant Devices.
Rights Object	A collection of Permissions and other attributes which are linked to Protected Content.
Superdistribution	A mechanism that (1) allows a User to distribute Protected Content to other Devices through potentially insecure channels and (2) enables the User of that Device to obtain a Rights Object for the superdistributed Protected Content.
Transfer	To relocate Protected Content or a Rights Object from one place to another.
Unprotected Content	Content which is not Protected Content.
User	The human user of a Device. The User does not necessarily own the Device.

3.3 Abbreviations

3GPP	3rd Generation Partnership Project
CD	Compact Disc
CEK	Content Encryption Key
DCF	DRM Content Format
DRM	Digital Rights Management
DVD	Digital Versatile Disc
HTTP	HyperText Transfer Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
MMS	Multimedia Messaging Service
MPEG	Motion Picture Expert Group
MP3	MPEG audio layer 3; coding scheme for audio compression
OMA	Open Mobile Alliance
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
REK	Rights Encryption Key
RFC	Request For Comments
RI	Rights Issuer
RO	Rights Object
SCR	Static Conformance Requirement
SIM	Subscriber Identity Module
SMS	Short Messaging Service
UI	User Interface
URI	Uniform Resource Indicator

4. Introduction

The role of DRM in distribution of content is to enable business models whereby the consumption and use of content is controlled. As such, DRM extends beyond the physical delivery of content into managing the content lifecycle. When a user buys content, she may agree to certain constraints - for example by choosing between a free preview version or a full version at cost, or she may agree to pay a monthly fee. DRM allows this choice to be translated into permissions and constraints, which are then enforced when the user accesses the content.

4.1 Actors and Functional Entities

An actor is defined here as an external entity involved in carrying out use cases. There exist a large number of possible actors in a DRM system. Examples range from content owners, content developers and content distributors, via network service providers and billing service providers, to manufacturers of network equipment and devices, and finally consumers of content. Depending on deployment scenario, different actors can play different roles in the system.

In the OMA DRM architecture, functional entities are used to embody specific roles in the DRM system. This makes it possible to decompose the tasks involved in digital rights management, separately from what actors perform each task in a certain deployment.

The functional entities are logical and need not represent physical network nodes (servers, etc). Depending on configuration, different functional entities may be implemented by the same or different physical nodes, and be operated by the same or different actors. Different deployments may incorporate some or all of the functional entities depending on the required functionality in each deployment setting.

From the point of view of digital rights management, the following functional entities have been identified in the architecture:

- DRM Agent

A DRM agent embodies a trusted entity in a device. This trusted entity is responsible for enforcing permissions and constraints associated with protected content, controlling access to protected content, etc.

- Content Issuer

The content issuer is an entity that delivers protected content. OMA DRM defines the format of protected content delivered to DRM agents, and the way protected content can be transported from a content issuer to a DRM agent using different transport mechanisms. The content issuer may do the actual packaging of protected content itself, or it may receive pre-packaged content from some other source.

- Rights Issuer

The rights issuer is an entity that assigns permissions and constraints to protected content, and generates rights objects. A rights object is an XML document expressing permissions and constraints associated with a piece of protected content. Rights objects govern how protected content may be used – protected content cannot be used without an associated rights object, and may only be used as specified by the rights object.

- User

A user is the human user of protected content. Users can only access protected content through a DRM agent.

- Off-device Storage

Protected content is inherently secure, and may be stored by users off-device - for example in a network store, a PC, on removable media or similar. This may be used for backup purposes, to free up memory in a device, and so on. Similarly, rights objects that only contain stateless permissions may be stored off-device.

4.2 Functional Architecture

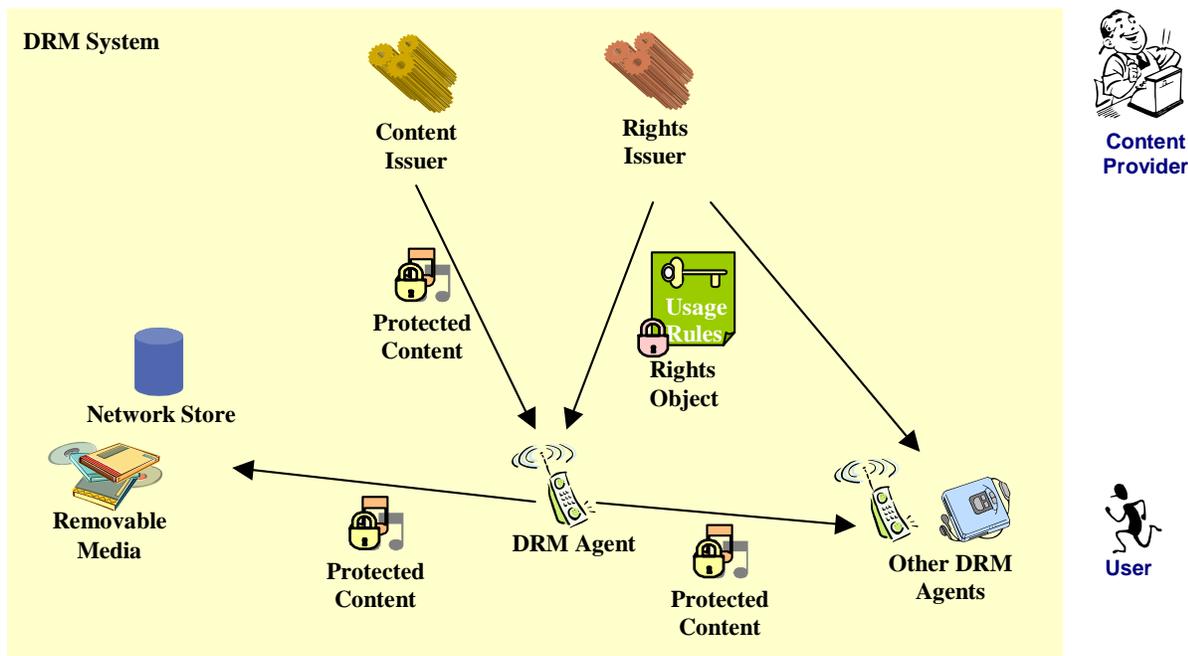


Figure 1. Functional architecture.

Before content is delivered, it is packaged to protect it from unauthorised access. A content issuer delivers protected content, and a rights issuer generates a rights object. The content issuer and rights issuer embody roles in the system. Depending on deployment they may be provided by the same or different actors, and implemented by the same or different network nodes. For example, in one deployment, content owners may pre-package protected content, which is then distributed by a content distributor acting as both content issuer and rights issuer.

A rights object governs how protected content may be used. It is an XML document specifying permissions and constraints associated with a piece of protected content. Protected content cannot be used without an associated rights object, and may only be used according to the permissions and constraints specified in a rights object.

OMA DRM makes a logical separation of protected content from rights objects. Protected content and rights objects may be requested separately or together, and they may be delivered separately or at the same time. For example, a user can select a piece of content, pay for it, and receive protected content and a rights object in the same transaction. Later, if the rights object expires, the user can go back and acquire a new rights object, without having to download the protected content again.

Rights objects associated with protected content have to be enforced at the point of consumption. This is modelled in the OMA DRM specifications by the introduction of a DRM agent. The DRM agent embodies a trusted component of a device, responsible for enforcing permissions and constraints for protected content on the device, controlling access to DRM protected content on the device, and so on.

A rights object is cryptographically bound to a specific DRM agent, so only that DRM agent can access it. Protected content can only be accessed with a valid rights object, and so can be freely distributed. This enables, for example, superdistribution, as users can freely pass protected content between them. To access protected content on the new device, a new rights object has to be requested and delivered to a DRM agent on that device.

The OMA DRM specifications define the format and the protection mechanism for protected content, the format (expression language) and the protection mechanism for the rights object, and the security model for management of encryption keys. The OMA DRM specifications also define how protected content and rights objects may be transported to devices using a range of transport mechanisms, including pull (HTTP Pull, OMA Download), push (WAP Push, MMS) and streaming. Any interaction between network entities, e.g. between rights issuer and content issuer, is out of scope.

4.3 Technical Use Cases

OMA DRM is designed to be flexible and support a wide variety of different business and usage models. This section outlines some technical use cases covered by the specifications. It is not an exhaustive list.

4.3.1 Basic Pull Model

A user selects content to download by browsing to some web site, and confirms the terms of the purchase. The content issuer identifies and protects content (packaging). Device capabilities can be detected using advertised MIME-type support, UAProf, etc.

The rights issuer generates a rights object for the content and the target DRM agent. A rights object includes permissions appropriate for the transaction.

Finally, the rights object is protected in a way that makes the protected content accessible only to the target DRM agent.

Protected content and the protected rights object are then delivered to the DRM agent.

4.3.2 Push of Protected Content

The basic scenario outlined above is based on a user initiated pull model. An alternative distribution model is to push content directly to a device using MMS, WAP Push or similar, without a preceding discovery process. There are two basic variations on this model:

- Content Push

The content issuer/rights issuer may have some previous knowledge of a user and a particular DRM agent, so that content and a rights object can be correctly formatted and packaged for delivery. For example, the user may have registered to receive a daily background image to her phone, or the hit song of the week. In this case the process would go through the same steps as above, but delivery of protected content and rights objects would be over WAP Push or MMS.

- Push-initiated Pull

In this case, the content issuer/rights issuer has no previous knowledge of a user or the target DRM agent, but still wishes to send content. For example, one user may buy some content as a gift to another user. In this case, the content provider does not yet know what content is suitable for the receiving device, how trusted the receiving DRM agent is, and so on. Instead of pushing protected content directly, a link to the content can be sent. Following the link will take the receiving user to a specific location, and then the procedure continues as in the basic pull model.

4.3.3 Streaming of Protected Content

The two previous examples assume that content is packaged and delivered in its entirety. Alternatively, content may be packetised and delivered as a stream.

In this case, the stream itself is protected (encrypted). OMA DRM does not specify formats for encrypted streams as other standards bodies are specifying this. Streams may be protected with encryption schemes which are different from those specified by OMA for Download, to address possible packet loss, etc. Once the stream has been encrypted, access to it can be controlled through the same procedure as described earlier for non-streamed content. A rights object is generated, the encryption key(s) to access the encrypted stream is put in the RO just like a CEK would, and the RO is then bound to a DRM agent. Without the rights object, the protected stream cannot be accessed.

4.3.4 Backup

Protected content can be stored safely on removable media, in a network store, or in some other form of storage. Protected content is stored in encrypted form, and so can only be accessed by a particular target DRM agent using an associated rights object.

Copies of rights objects can be created for backup purposes and stored off-device, if the rights object only contains stateless permissions. The security model ensures that the rights object is protected and can only be accessed by the intended DRM agent – even if a rights object is stored off-device, it will still only allow the intended DRM agent to access associated protected content.

Some permissions require maintenance of state by the DRM agent, for example a limited number of plays. Such rights objects cannot be copied or stored off-device, as this might result in loss of state information - e.g. current number of plays. A lost or damaged rights object may still be restored via the rights issuer by requesting a new rights object.

4.3.5 Super Distribution

Protected content can be safely copied and transferred to other DRM agents, for example a user sending protected content to a friend. In order to access protected content, the friend is taken to the rights issuer, by way of a link in the protected content package, to acquire a rights object. The rights issuer controls whether to release a new rights object or not to the new DRM agent.

4.3.6 Export

Protected content may be exported to other DRM systems, for use on devices that are not OMA DRM compliant but support some other DRM mechanism – e.g. export to copy protected media. The rights issuer may limit export only to specific external DRM systems.

The OMA DRM architecture allows rights issuers to, if they wish, express permission for DRM agents to perform conversions to specific other DRM systems. It is expected that other DRM systems will specify how such a conversion is done.

Devices supporting export to other DRM systems must ensure that the content remains protected throughout the export process.

4.3.7 Store and Forward

OMA DRM supports delivery models using intermediary devices.

For example, a user has an OMA DRM compliant portable device, and a PC. She uses the PC to browse and purchase content, and receives protected content to the PC. She then transfers the protected content to her OMA DRM compliant mobile device over a local connection. The DRM agent on the device requests and downloads rights objects from the rights issuer, but does not have to download the content objects again.

Using intermediaries in this way can be useful if the target device has a limited UI, or to allow the user to download content objects over broadband connections and only download rights objects over the air. Only the target device needs to be OMA DRM compliant.

5. Trust and Security Model

The fundamental challenge facing any DRM solution is how to ensure that permissions and constraints associated with protected content are enforced. The main threat comes from unauthorised access to protected content beyond what is stipulated by the associated rights objects, or creation of illegal copies and redistribution of valuable content such as music and games.

Rights objects and DRM protection are enforced at the point of consumption. This is modelled in the OMA DRM specifications by the introduction of a DRM agent. The DRM agent embodies a trusted environment within which protected content can be securely consumed. Its role is to enforce permissions and constraints and to control access to protected content.

5.1 Overview

The basic steps for distributing protected content can be summarised as follows:

1. Content packaging: Content is packaged in a secure content container (DCF). Protected content is encrypted with a symmetric content encryption key (CEK). Content can be pre-packaged, i.e. content packaging does not have to happen on the fly.

Although not required by the OMA DRM specifications or the OMA DRM architecture, it is recommended that the same CEK is not used for all instances of a piece of content. Using the same CEK for all content instances would pose a greater risk if a single device was to be hacked and a CEK stored on that device exposed. Using a different CEK for different deliveries or different devices will limit this risk.

2. DRM agent authentication: All DRM agents have a unique private/public key pair and a certificate. The certificate includes additional information, such as maker, device type, software version, serial numbers, etc. This allows the content and rights issuers to securely authenticate a DRM agent. Any privacy aspects with releasing such information are addressed in the technical specifications.
3. Rights Object generation: A rights object is an XML document, expressing the permissions and constraints associated with the content. The rights object also contains the CEK – this ensures that protected content cannot be used without an associated rights object.
4. Rights Object protection: Before delivering the rights object, sensitive parts are encrypted (e.g. the CEK), and the rights object is then cryptographically bound to the target DRM agent. This ensures that only the target DRM agent can access the rights object and the protected content

In addition, the RI digitally signs the RO.

5. Delivery: The RO and DCF can now be delivered to the target DRM agent. Since both are inherently secure, they can be delivered using any transport mechanism (e.g. HTTP/WSP, WAP Push, MMS). They can be delivered together, e.g. in a MIME multipart response, or they can be delivered separately.

5.2 Trust Model

The DRM agent has to be trusted by the rights issuer, both in terms of correct behaviour and in terms of a secure implementation. In OMA DRM, each DRM agent is provisioned with a unique key pair, and an associated certificate, identifying the DRM agent and certifying the binding between the agent and this key pair. This allows rights issuers to securely authenticate the DRM agent using standard PKI procedures.

The information in the certificate enables the Rights Issuer to apply a policy based on its business rules, the value of its content, etc. For example, a rights issuer may trust certain manufacturers, or it may keep an updated list of DRM agents that are known to be good or bad according to some criteria defined by the rights issuer. It is also possible for a group of stakeholders to establish a joint authority identifying trusted DRM agents, with legally binding compliance rules.

Revocation in this model amounts to not distributing content any more to DRM agents that are no longer considered trusted. What constitutes a trusted DRM agent depends on the policy and business model of rights issuers. For example, if a hack or a

fault compromises a whole class of devices, a rights issuer may decide to stop distributing new content to all devices of that type or class. This is a worst-case scenario. At the other end of the spectrum, maybe there is a known bug in devices of a certain type, but the risk of content leaking is relatively small. In such cases, content and rights issuers may choose to continue to deliver content to existing devices, and instead let manufacturers correct the problems in future versions. Either way, the secure mechanism for authenticating DRM agents enables rights issuers to enforce such policies.

5.3 Content Protection

The DRM Content Format (DCF) is a secure content package for encrypted content, with its own MIME content type. In addition to the encrypted content it contains additional information, such as content description (original content type, vendor, version, etc.), rights issuer URI (a location where a rights object may be obtained), and so on. This additional information is not encrypted and may be presented to the user before a rights object is retrieved.

Since a DCF is inherently secure, it can be transported using any transport protocol, e.g. in an HTTP response or in an MMS message. It can be stored for back-up on any kind of storage, e.g. removable media or a networked PC. It can be copied and sent to another DRM agent, where a rights object may be acquired for use on the receiving device (superdistribution).

The content encryption key needed to unlock protected content inside a DCF is contained within a rights object. Thus it is not possible to access protected content without a rights object. Protected content can only be used as specified in a rights object.

OMA DRM includes a mechanism allowing a DRM agent to verify the integrity of a DCF, protecting against modification of the content by some unauthorised entity.

5.4 Rights Object

Rights objects are used to specify consumption rules for protected content. The Rights Expression Language (REL) defined by OMA DRM specifies the syntax (XML) and semantics of permissions and constraints governing the usage of protected content. An instance of a rights document is called a rights object, and has its own MIME content type.

Rights objects are made up of permissions (e.g. play, display and execute) and constraints (e.g. play for a month, display ten times). Rights objects may also include constraints that require a certain user (user identity) to be present when the content is used. These permissions and constraints, along with other information embodied in the rights object, (e.g. copyright information) may be presented to the user. The rights object also governs access to protected content by including the content encryption key (CEK).

A single rights object may be associated with multiple pieces of protected content. Further, it is possible to assign different permissions to different components of a composite object.

Conversely, a single piece of protected content may be associated with multiple rights objects. If there are multiple rights objects associated with a piece of protected content, each rights object is treated individually – rights objects are not combined. This means that at any one time, there may be more than one rights object whose constraints are satisfied. When this is the case, the DRM agent selects one to enforce. This selection may be made automatically by the DRM agent based on some selection criteria, e.g. picking the least restrictive rights object, or it may be done based on user interaction.

5.5 Rights Object Protection

A rights object is protected using a rights encryption key (REK). The REK is used to encrypt sensitive parts of the rights object, such as the CEK. In addition, the RO is digitally signed by the RI.

During delivery, the REK is cryptographically bound to the target DRM agent. In this way only the target DRM agent can access the rights object, and thus the CEK.

Since a protected rights object is inherently secure, it can be copied and stored off-device for backup purposes. Some permissions require maintenance of state by the DRM agent, for example a limited number of plays. Rights objects containing such permissions cannot be copied or stored off-device, if this would result in loss of state information - e.g. current number of plays.

5.6 Other Security Aspects

The building blocks described above address the main security issues of protecting content and rights objects from unauthorised access. In addition, OMA DRM addresses a number of other security aspects, including:

- Rights Issuer Authentication

Rights issuers are required to authenticate themselves to the DRM agent during delivery of rights objects. This gives some level of assurance about the authenticity of the rights issuer.

- Rights Object Replay Protection

An example of rights object replay would be if an intermediary intercepts a rights object with a limited number of plays during delivery to the DRM agent. When the rights run out on the DRM agent, the intercepted rights object might be delivered again (replayed) from the intermediary. OMA DRM prevents this and similar attacks from occurring.

- Secure Time

Some constraints (absolute time constraints), as well as some aspects of the delivery protocol for rights objects, rely on the DRM agent having a secure time source. Secure time in the context of the OMA DRM specifications means accurate as well as not changeable by users. Since users are not able to change the DRM agent time, the OMA DRM specifications provide mechanisms for the DRM time to be synchronised when necessary, e.g. if time is lost after prolonged power failure.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version

A.2 Draft/Candidate Version 2.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-DRM-ARCH-V2_0	09 Sept 2003		Initial public draft